REAL TIME ANALYSIS: DOES NAVY HAVE A PLAN?

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

GARY M. OLIVI, LCDR, USN
B.S., US Naval Academy, Annapolis, Maryland, 2000

Fort Leavenworth, Kansas
2015

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 12-06-2015	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From - To)* AUG 2014 – JUN 2015

4. TITLE AND SUBTITLE Real Time Analysis: Does Navy Have a Plan?	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) LCDR Gary M. Olivi	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301	**8. PERFORMING ORG REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

US Navy Information Dominance (ID) continues to rely on the collection of as much information as possible from the electromagnetic and cyber domains to conduct operations. However, with the increase in organic sensor data along with access to information that was currently outside Navy channels, data overload threatens the ability of the Navy to perform real time analysis. In the past three years the Navy ID community has chartered multiple roadmaps and vision documents nested within national policy to lead the way for decision superiority based on the information collected in the electromagnetic and cyber domains.

As the Navy ID strategies begin to unfold into physical tasking the Navy needs to ensure the ID organization is aligned correctly to assist with the analysis of information gathered, innovation of the organization and leveraging the right commercial technology. With the military services operating under austere budgetary constraints and the rise of nefarious state and non-state actors acquiring low cost threat weapons, Navy ID has no room for failure. Navy ID needs to ensure they have constant home field advantage with their capabilities while operating forward from the sea.

15. SUBJECT TERMS
Real Time, Analysis, Information Dominance, Strategy, Maritime, United States Navy, SIGINT, Cyber

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT (U)	**b. ABSTRACT** (U)	**c. THIS PAGE** (U)	(U)	69	**19b. PHONE NUMBER** *(include area code)*

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: LCDR Gary M. Olivi

Thesis Title: Real Time Analysis: Does Navy Have a Plan?

Approved by:

____, Thesis Committee Chair
Jack D. Kem, Ph.D.

____, Member
LTC Ryan D. Strong, B.S.

____, Member
Brian G. Blew, M.S.

Accepted this 12th day of June 2015 by:

____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

REAL TIME ANALYSIS: DOES NAVY HAVE A PLAN? by LCDR Gary M. Olivi, 69 pages.

US Navy Information Dominance (ID) continues to rely on the collection of as much information as possible from the electromagnetic and cyber domains to conduct operations. However, with the increase in organic sensor data along with access to information that was currently outside Navy channels, data overload threatens the ability of the Navy to perform real time analysis. In the past three years the Navy ID community has chartered multiple roadmaps and vision documents nested within national policy to lead the way for decision superiority based on the information collected in the electromagnetic and cyber domains.

As the Navy ID strategies begin to unfold into physical tasking the Navy needs to ensure the ID organization is aligned correctly to assist with the analysis of information gathered, innovation of the organization and leveraging the right commercial technology. With the military services operating under austere budgetary constraints and the rise of nefarious state and non-state actors acquiring low cost threat weapons, Navy ID has no room for failure. Navy ID needs to ensure they have constant home field advantage with their capabilities while operating forward from the sea.

ACKNOWLEDGMENTS

I wish to extend my sincere gratitude to the members of my thesis committee: Dr. Jack Kem, LTC Ryan Strong, and Mr. Brian Blew. Their knowledge, guidance, and patience throughout this process was integral to the successful completion of this project. Their mentoring and constructive feedback greatly improved my critical thinking, research, and writing skills. The time and effort they devoted to guide my efforts positively impacted the final product; I am truly grateful.

My deepest appreciation goes out to my bride of 13 years, Lori, and our son Tyler for their tireless encouragement, prayer support, and sacrifice. Lori definitely had the harder job out of the two of us this year, while I went to school and she held down the fort. Their unconditional love, administered long distance, ensured I never felt alone or overwhelmed throughout the process and they always cheered me up on tough days.

TABLE OF CONTENTS

ACRONYMS

ID	Information Dominance
IDC	Information Dominance Corps
ISR	Intelligence Surveillance Reconnaissance
JOAC	Joint Operational Access Concept
NDS	National Defense Strategy
NMDAP	National Maritime Domain Awareness Plan for the National Strategy for Maritime Security
R&D	Research and Development
SIGINT	Signals Intelligence
TYCOM	Type Commander

ILLUSTRATIONS

Page

TABLES

CHAPTER 1

INTRODUCTION

> Control of information-much of it through the electromagnetic spectrum–is already growing more important than the control of territory in modern warfare.
> — Admiral Jonathan Greenert, quoted in *Navy Strategy for Achieving Information Dominance, 2013-2017*

Background

The US Navy's ability to stay ahead of the adversary and respond to crises has become more challenging than at any given time period. As it faces a new, more capable threat from state and non-state actors, the Navy must change the way it operates from within. These new threats are acquiring new low cost technology to implement new tactics, techniques and procedures. Meanwhile the Navy operational budget continues to decrease. In order to meet this challenge the Navy will need to innovate both organizationally and through technology to meet their objectives.

In 2009, the US Navy brought its core information centric disciplines (Information Warfare, Intelligence, Information Professional, Oceanography and Space Cadre) under one common umbrella called the Information Dominance Corps (IDC). The thought in 2009 as many have heard, is that knowledge is power, and these core disciplines were the main body that gave US Navy her power. This change built an inter-disciplinary corps from communities that previously leveraged one another when needed, and created an information powerhouse if developed together.

This organizational change enabled the Navy to collect, process, and exploit intelligence at a much faster pace and discover more data in order to make smarter faster decisions. Naval leadership understood the need for rapid innovation while needing to maintain present Information Dominance (ID) capabilities. Therefore, they began to rethink how they would reorganize and correctly align their platforms, networks, and sensors to acquire the data they needed to make informed decisions for kinetic and non-kinetic operations.

In a 2012 article Admiral Greenert, Chief of Naval Operations stated, "We need to detect, assess, and predict in real time the activities going on in that domain, (EMS and cyber space), and use that knowledge to guide our own EM-cyber operations" (Greenert 2012, 18). In the same article, Admiral Greenert also commented on the Navy's current ability to collect and analyze when he stated:

> Today we understand how weather, geography, and other EM emissions can affect EM signals, and we are developing improved techniques to identify computer-network anomalies that may indicate threats or potential threats. But our tools for collecting and analyzing information in the EM-cyber environment are limited, and we lack the familiarity and understanding to take full advantage of what information we do have -often learning only in retrospect what happened in a particular jamming, communication, or cyber event and why it occurred. (Greenert 2012, 18)

The amount of big data that the Navy must process is growing more and more every second. In order to give a brief overview of what Navy ID is facing when it comes to getting their expertise in line with understanding the data for battlespace awareness we can look at a few highlights of big data in both the commercial world and organic to the Navy to comprehend the breadth of the problem.

The commercial world is producing the following:

> 90% of the world's data has been created in the past 2 years. (Progress Software Corporation 2014)

> By 2020, 35 zettabytes of data will have been created and one-third of this data will have been stored in or passed through a cloud. (Progress Software Corporation 2014)
>
> Everyday 2.5 Quintillion bytes of data are generated by people. (Progress Software Corporation 2014)
>
> China will account for more than one-fifth of the world's data by 2020. (McCafferty 2014)
>
> 70% of the digital universe-900 exabytes-is generated by users. (McCafferty 2014)

Over the next decade, the Navy is growing their organic sensor capability that will add to their ability to analyze their organic data as their growth is depicted in figures 1 and 2.

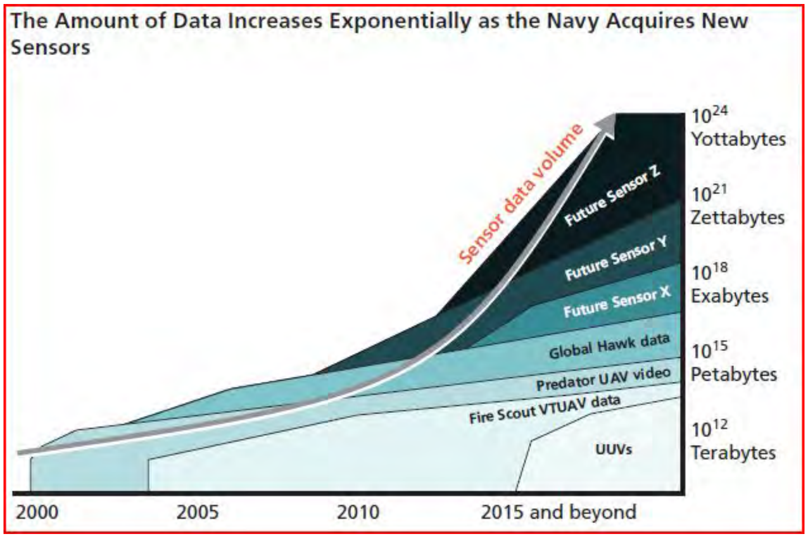


Figure 1. Future Data Growth for the US Navy

Source: Isaac Porsche, *Data Flood: Helping the Navy Address the Rising Tide of Sensor Information* (Santa Monica: RAND Corporation, 2014), 5.

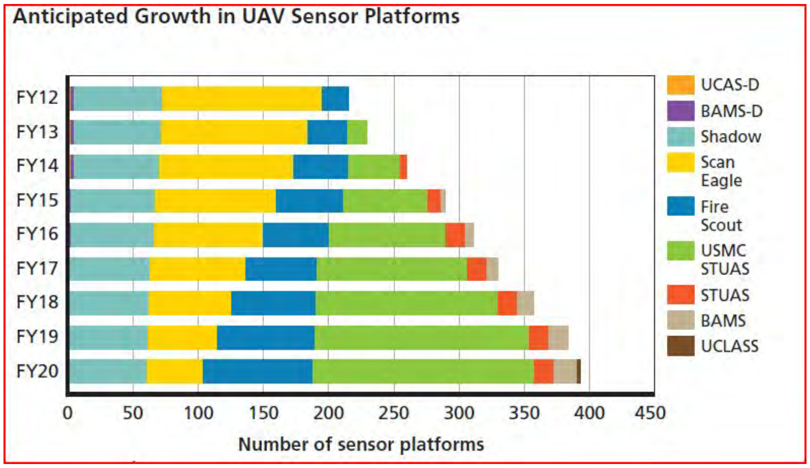


Figure 2. Probable Unmanned Aerial Vehicle Sensor Growth in US Navy

Source: Kendall Card, "Navy ISR Family of Systems: An Integrated Future," (Presentation at Navy Information Dominance Industry Day, Chantilly, VA, March 7, 2012).

Because of this growth, the Navy must have a sound and solid ID strategy to deal with the adversarial threats that are roaming the global commons. For this reason, the Navy has released four ID roadmaps and strategies into the workforce over the past two years dealing with electromagnetic spectrum and cyberspace and how the Navy will align to meet these challenges.

Primary Research Question

Is Navy ID implementing the correct strategy with all their platforms, sensors, and networks interconnected to ensure decision superiority through robust analysis of data?

Secondary Research Questions

Secondary research questions that arise from the primary research question are:

1. Does having more data accessible to a naval unit allow for an easier management of sensor employment against requirements and enhanced Battlespace Awareness?
2. Is current technology available now that the Navy ID should be leveraging?
3. Does the current Navy ID strategy assist or hinder the naval analyst in viewing the battlespace?

Significance

This research will look into how Navy ID is aligning their priorities to meet the operational goals laid out within their strategic and operational documents for ID. The importance of this study is to help determine if priorities are aligned correctly and to see if any key pieces of strategy are missing or incorrectly defined setting a course for Navy ID failure. If a critical piece of information is missing from current strategy this research may help in recommending solutions for that problem.

Assumptions

The speed at which warfare is conducted will continue to increase through the spread of low cost information technology. The amount of available data will continue to increase because of larger use of the electromagnetic spectrum and cyber domains. Navy's ID will continue focus on the three areas laid out in their strategic documents:

Assured Command and Control

Battlespace Awareness

Integrated Fires (Card and Rogers 2012c, 3)

Definitions and Key Terms

The following terms will be used throughout this study:

Assured Command and Control: The Navy must assure its ability to command and control forces. This requires capabilities that enable commanders to exchange orders and responses with subordinates, understand the disposition of friendly forces, target and conduct strikes as part of the joint force and assess the result of those strikes (Card and Rogers 2012c, 6).

Battlespace Awareness: Persistent surveillance of the maritime and information battlespace, penetrating knowledge of the capabilities and intent of our adversaries, an understanding of when, where, and how our adversaries operate and expertise in the electromagnetic spectrum. When synchronized, these skills and knowledge attributes provide the target acquisition and targeting solutions necessary to apply force, both kinetic and non-kinetic (Card and Rogers 2012c, 7).

Big Data: Big data is a constantly moving term. It can range from petabytes to terabytes depending on which forum it is being discussed. For the purpose of this research, the Big Data will be used as described in the *International Journal of Internet Science* which is data sets with sizes beyond the ability of commonly used software tools to capture, curate, manage, and process the data within a tolerable elapsed time (Snijders, Matzat, and Reips 2012, 1).

Information Dominance: The operational advantage gained from fully integrating the Navy's information functions, capabilities, and resources to optimize decision making and maximizing warfighting effects.

Integrated Fires: The Navy will use its networks, cyberspace, and space capabilities to exploit and attack vulnerabilities of its adversaries to achieve non-kinetic effects. Just as importantly, Navy will expand options for forward-deployed Navy commanders by ensuring non-kinetic alternatives are considered alongside with kinetic solutions (Card and Rogers 2012c, 7).

Maritime Domain Awareness: An effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States.

Predictive Analytics: Predictive analytics helps your organization predict with confidence what will happen next so that decision makers can make smarter decisions and improve outcomes.

Real Time Analysis: This research will define Real Time Analysis as analysis done within sixty seconds.

Real Time Collection: This research will define Real Time Collection as collection done within sixty seconds.

Limitations

The main limitation is the continually changing information technology environment. This study will compile research over approximately eight months. The advances in information technology are changing rapidly so by the time this thesis is published, there may have been advances that this thesis did not observe and could not reflect on in this thesis.

The Navy ID strategy and vision has only been distributed since 2010, shortly after the creation of the IDC. Since not enough time has elapsed for full implementation of the strategy, this study will be limited by the implementation that has occurred to date.

Scope and Delimitations

This study will assess the suitability and feasibility of Navy's ID strategy for gaining decision superiority through analysis of data. Research for this study was conducted with a specific focus on Navy ID strategy. This study will not address any challenges to the other military services or the joint forces. This study will not assess the threats that challenge naval air, sea, space, and cyber space domains.

This study was intentionally done at the unclassified level and does not seek to provide answers in the classified domain. Since the study was done at the unclassified domain, it will not seek technical solutions being provided in the classified realm.

Conclusion

Determining whether the US Navy ID community is headed toward becoming a success by looking into its policy, organizational structure, and technology implementation will allow for gaps in any of the major parts to be determined. If gaps are discovered it will then assist in providing recommendations on how to mitigate those areas. The ability of being able to sift through large volumes of data to give the operational commander decision superiority is being espoused in all services and strategic policy while defense budget cuts are making this task a much greater problem set than any time before due to the adversaries use of the electromagnetic spectrum and cyber domains.

Chapter 1 introduced the background of the thesis, explained the problem, and why it is important to navy leaders. The first chapter also provided the overview of the thesis in the form of primary and secondary research questions, the thesis assumptions, its limitations, and delimitations so the reader knows what will be covered. Chapter 2 categorizes the literature to provide a framework for what was studied. Chapter 3 describes the methodology used to conduct the research to enable the reader's understanding of the research design and why this particular methodology is appropriate for this research. Chapter 4 uses the methodology to analyze the problem in order to determine where gaps are in the Navy ID organization. Chapter 5 provides insights and interpretations of the data from the previous chapter and offers recommendations to mitigate any perceived problems and areas needing further research.

CHAPTER 2

LITERATURE REVIEW

Introduction

The purpose of this literature review is to evaluate existing literature relevant to Navy ID in implementing the correct strategy to ensure decision superiority through robust analysis of data. This chapter will also assist in determining any significant issues hindering the Navy's ID strategy from succeeding and will break the research into four areas: (1) National strategy and policy pertinent to the Navy ID; (2) Current strategy and articles released by the Navy ID community over the last four years; (3) Current commercial technology trends that could assist the Navy ID community in succeeding at their goals; and (4) Problems that are appearing with big data as it relates to the Navy.

National Strategy

In reviewing national strategy that the Navy ID community must align with, there are ample resources that discuss the need for a greater understanding of the battlespace and ability to fuse intelligence and make decisions in real time. The order to complete the aforementioned task has been highlighted in several of our armed forces strategic guiding documents.

In the *National Defense Strategy 2012* (NDS), President Barack Obama highlighted the need to prevail in the cyber domain. This presidential document outlines the objectives that our military services must strive to accomplish. The impact of signaling out the cyber domain over air, land, sea, and space sends a key message to our military.

There are three key parts in the NDS that have a direct impact on how Navy must shape their force and deeper into the Navy, how Navy ID must shape its workforce and decision making skillsets. The first part in NDS that highlights this need is the passage under the Global Security Challenges where it states "The United States will continue to lead global efforts with capable allies and partners to assure access to and use of the global commons, both by strengthening international norms of responsible behavior and by maintaining relevant and interoperable military capabilities" (US President 2012, 3). For the Navy to lead in sustaining responsible use of the global commons and protect the use of space and cyber-space, it will need to change how they organize internally to deal with decision making against bad actors in the global commons. A nefarious bad cyber actor only needs a connection to a network to impact the global commons and the Navy, being forward deployed to these hostile areas, needs to prevail at deterring these events.

The next area that NDS highlights is the ability to project power even when facing anti-access/area denial challenges. The adversaries' asymmetric use of the electromagnetic spectrum and cyber domain cannot prevent our US Navy's use of her kinetic and non-kinetic instruments of power. This passage in the NDS has led to the *Air-Sea Battle: Service Collaboration to Address Anti-Access and Area Denial Challenges* and the *Joint Operational Access Concept* (JOAC) that will impact how the US Navy must focus its forces.

Lastly, the final piece of the NDS that directly affects US Navy ID is to operate effectively in space and cyberspace. This has more to do with the need for reliable information and the ability to act on the reliable information. With increased threats to communication networks, space assets, and weapon systems the ability to conduct high tempo effective operations rests with the ability to use the information we collect to defend, adapt and stay resilient (US President 2012, 5).

These three pieces of the NDS make it clear how important it is to have large amounts of information, which is reliable to act on, in order to strengthen our nation's capabilities to defend and deter adversaries. The US Navy will need to ensure they are building a capable workforce that can handle these tasks.

The JOAC is aimed at achieving operational access, the ability to project military force into an operational area, to support a series of broad strategic goals, including ensuring access to commerce, demonstrating US resolve to manage a crisis or prevent war, or defeating an enemy. The idea is for military decision makers to think through the problems ahead of time. It has been universally recognized in our US military that our greatest challenges foreshadowed in the future will be from adversaries who have the ability to deny US military forces our stand alone combat power. This challenge can only be negated if the services work jointly to defeat these threats (JCS 2012, 1).

The JOAC references having a formidable understanding of all the effects of each US military service's capability so that the commander can be more aware of how the use of a weapon or tactic in one domain would impact the other warfighting domains. Taking this type of approach also allows for commanders to be more aware of what the different capabilities are in each military service to use them in a greater capacity.

The ability to understand what the possible second and third order effects are for each capability used and what assets are available to use will not come about simply by merging the services into this construct. One will need to merge the networks, data sharing capabilities, command and control, visualizations, etc. in order to have a greater awareness of the capabilities and their effects. JOAC also highlights several of the main capabilities being the ability to conduct timely and accurate cross-domain all-source intelligence fusion in an opposed access situation. The ability to develop all categories of intelligence in any necessary domain in the context of opposed access and the ability to leverage cross-domain cueing to detect and engage in-depth to delay, disrupt, or destroy enemy systems (JCS 2012, 34).

With those capabilities the JOAC in its fullest form is resource intensive and could be economically unsupportable (JCS 2012, 37). This will require the need to sift through large amounts of data within each service's repository and ensure the golden nuggets are being pulled from the data correctly, shared in the appropiate manner in order to analyze the battlespace fully. The commander will not have time to judge the information and will need to make a decision on the data being analyzed instantly. This increases the need to ensure all the data is being vetted and connected to the appropiate puzzle pieces needed for the commander's decision.

Air-Sea Battle centers on networked, integrated, attack-in-depth to disrupt, destroy and defeat anti-access/area denial (Air-Sea Battle Office 2013, 4). This approach exploits and improves upon the advantage US forces have across the air, maritime, land, space, and cyberspace domains, and is essential to defeat increasingly capable intelligence gathering systems and sophisticated weapons systems used by adversaries employing anti-access/area denial systems. Offensive and defensive tasks outlined in *Air-Sea Battle* are tightly coordinated in real time by networks able to command and control air and naval forces in a contested environment. The air and naval forces are organized by mission and networked to conduct integrated operations across all domains.

The Air-Sea Battle concept desires to have a networked force with people and equipment linked in time and purpose with interoperable procedures; command control structures; and appropriate authorities capable of translating information into actions (Air-Sea Battle Office 2013, 6).

The reference above alludes to the fact that the services operating under this concept will have the capability to translate mass amounts of data between people and system. However, *Air-Sea Battle* makes no mention of how any of the services should go about building or leveraging the information data fusion capabilities. As *Air-Sea Battle* will be a strategic document to help shape how US Navy ID needs to be aligned, it gives very little on where the focus should be.

The *National Maritime Domain Awareness Plan for the National Strategy for Maritime Security* (NMDAP) is one document that has an effect on how Navy ID needs to shape their strategy on maritime domain awareness. NMDAP supports Presidential Policy Directive-18 and supports the promotion of a secure and responsible decision-making body across all levels of global maritime community of interest.

NMDAP specifically highlights under their first goal for the strategy the significance of data for decision-making superiority. NMDAP states, "the purpose of MDA [Maritime Domain Awareness] is to facilitate timely, accurate, and informed decision-making. Decision-makers require timely, accurate, and relevant information to successfully prepare for, prevent, respond to, and recover from threats" (US President 2013, 10).

NMDAP continues to highlight different aspects of maritime domain awareness, with the majority of them focusing on intelligence sharing, fusion of data, and timely collection and analysis on the data. This strategy will be useful to not just the US Navy, but to the US Navy ID community's closest partners to include Commander Tenth Fleet, Office of Naval Intelligence, Office of Naval Research, and multiple other intelligence agencies that have an interest in the maritime.

NMDAP has already sparked the US maritime community to develop a Maritime Information Sharing Environment, directed by the Office of Naval Intelligence, that not only supports the tasking laid out in NMDAP, but the NDS and JOAC required capabilities as well. The goal of this new endeavor is to ensure the right people have the right data at the right time to make the right decision.

Navy Information Dominance Corps Vision

In November 2012, Navy ID leadership signed three documents to guide how Navy ID will be shaped to grow internally and be ready to deal with the threats on the horizon that the Navy will be facing. The first of these documents, *Navy Strategy for Achieving Information Dominance 2013-2017,* is the overarching strategy from which the other documents on this topic have been developed.

The strategy focuses on the three fundamental ID capabilities of Assured Command and Control, Battlespace Awareness, and Integrated Fires, and sets forth the following major goals for the 2013–2017 timeframe:

- Strong and Secure Navy Command and Control;
- Persistent, Predictive Battlespace Awareness;
- Integrated Combat Information;

• Integrated Kinetic and Non-kinetic Fires;

• Information Dominance as a Warfighting Discipline. (Card and Rogers 2012c, 3)

Throughout this strategy, the objectives are laid out for accomplishing each goal to succeed at meeting the overarching capabilities needed. While several objectives reference the enormous amounts of data that will need to be managed and analyzed, no guidance is set forth on how to accomplish predictive analysis.

The Navy released *U.S. Navy Information Dominance Roadmap 2013-2028* in March 2013, outlining the challenges for operating in the information environment over the next fifteen years. The purpose of this document is to summarize the operating and information environments expected during the 2013-2028 timeframe and depict the Navy's required future ID capabilities. This roadmap focuses more on the long-term planning aspects necessitated by the anticipated changes to the information environment, but keeps the focus on the fundamental capabilities and goals outlined in *Navy Strategy for Achieving Information Dominance, 2013-2017.* This roadmap highlights the fact that Navy's efforts in the battlespace awareness area are hampered by unclear roles and responsibilities, Navy's capabilities do not allow for adequate information sharing and visualization, the Navy is being overwhelmed by the volume of sensor data being collected and that processing functions of this data being collected need to be enhanced (Leigher 2013, 15-16).

The roadmap continues to describe generic remedies for overcoming the obstacles mentioned above, but again it is more themes and ideas. Actual guidance that can be tasked to achieve the objectives highlighted in this roadmap on analysis and sensor management is greatly needed. This allows for commands to assume responsibility for completing these tasks.

Navy Cyber Power 2020 depicts how the Navy will accomplish their goals and objectives within the cyber domain. The vision laid out in this document is tied to the *Navy Strategy for Achieving Information Dominance, 2013-2017.* The three core capabilities in this vision are only different with the added word, cyber, but have the same end state.

- Assuring access to cyberspace and confident Command and Control
- Preventing strategic surprise in cyberspace
- Delivering decisive cyber effects (Card and Rogers 2012a, 1)

Strategic initiatives and tactical end states are laid out in this vision, a heavy focus on teaming with joint cyber forces, but it does not reference the volume of data the Navy ID community faces.

Navy Cyber Power 2020 strategic initiatives provide the ways and means to achieve and sustain the Navy's advantage in cyberspace (Card and Rogers 2012a, 9), but does not highlight the ways on which to achieve decision superiority through predictive analysis of the data only mentioning that situational awareness is needed.

The Navy ID community also issued the *Navy Information Dominance Corps Human Capital Strategy 2012-2017* roadmap on how it would employ its personnel to tackle their newest warfighting discipline and create a culture that enables the personnel to exceed in ID problem sets. The *Human Capital Strategy* details the training, experience, and tools needed for the personnel of the IDC.

The vision and goals of the *Human Capital Strategy* are similar and parallel the previous strategy and roadmaps reviewed earlier in this thesis, and it highlights the need for superior decision making throughout the Navy decision cycles. At every step of the decision cycles, Navy ID personnel need to play a critical role which is not built today. Currently, the steps needed for the personnel are convoluted, mismanaged, not educated to manage their roles, and encumbered by leadership to perform their duties that is why Navy ID senior leadership authored this document.

Current Technology Trends

The commercial world has been making the real time predicative analysis of big data one of their major priorities in the last few years. This is because in the commercial world, predictive analysis assists businesses with their bottom line. At this second, they are looking at all types of data to help them forecast what is needed on their part. Waiting days and weeks for an answer is not profitable, so it is logical that the commercial world is leading the way.

IBM is a current leader in analytics on big data. They are working with multiple Fortune 500 organizations on how to make sense of the companies' data being collected in real time and how to act in real time based on those analytics. In the majority of the literature that IBM has described their philosophy on real time analytics, it can be broken down into four parts:

> Analyze streaming data in real time as it flows through the organization.
>
> Make sense of unstructured data and put it into context with historical, structured data.
>
> Use predictive analytics and advanced algorithms to recommend actions in real time.

> Empower decision makers to act on insights in the moment, with confidence. (IBM Corporation 2014)

IBM has realized the impact that real time analytics has had on their organization and others in the ability to make better decisions. Furthermore, reviewing their products and solutions show little if any difference on what Navy ID needs for their data and analytics.

Automated Insights is a corporation that has made a dramatic change in the way one reads data using predictive analytics. They develop solutions to assist in how the data, when analyzed in real time, is reported in a natural form to be understood within the organizations' own culture. This is a new area of technology innovation, as no organization has the same culture language allowing for a generic solution that could be developed across the spectrum. Automated Insights transforms big data into written reports with the depth of analysis, personality, and variability of a human writer (Automated Insights 2014). This is helpful when decisions must be made instantly and decisions are not being made fast enough based on not having a common language.

Amazon is another company innovating the way analytics on big data is being done. They are developing software that can collect and process hundreds of terabytes of data per hour from hundreds of thousands of sources, allowing you to easily write applications that process information in real time, from sources such as web site click-streams, marketing and financial information, manufacturing instrumentation, and social media, as well as operational logs and metering data (Amazon 2014). These types of technology innovations assisted the Central Intelligence Agency in choosing a commercial provider to build their cloud services rather than trying to hobby shop their analytical needs in house (Konkel 2014).

The commercial sector is also looking at predictive analysis to determine unplanned equipment failures. This would coincide with the need for the Navy to be better at predicting when an engine on a ship or plane may fail unexpectedly or when a critical weapons system may malfunction. Accenture has begun incorporating predictive analytics on big data to predict when equipment will fail before it fails to reduce exepenses and operating cost of faulty equipment. Accenture uses the sensor data on the equipment to capture real time physical characteristics and comparing that data with optimal measurements. This allows for the company to apply mathematical models to predict the leading indicators of an unplanned breakdown. They follow a six step process: identify critical equipment, prioritize based on mission impact, determine root cause(s) of failure, create models used to predict failures, predict failures and optimize maintenance cost (Accenture Federal Services 2012).

This approach that Accenture uses also allows for better planning and inventory management which assists in increasing service. Navy ID is responsible for the protection of all sensor data from naval platforms, and might find a useful analytic in using an approach like Accenture for their platforms equipment on the data they collect.

Problems with Too Much Data

An article in the *Federal Times* gave a differing of opinions between commercial and military leaders within the intelligence community on how they viewed big data. The article speaks about the need to be able to find key facts of information throughout all the data being collected but highlights some concerns amongst the shared community.

Leadership in the military services recognizes problems with the amount of data needed for analysis. Captain Christopher Page, Deputy Director of Assured Command

and Control in the Office of the Deputy Chief of Naval Operations for Information Dominance said, “Big data’s potential has only begun to be tapped. At present, big data is viewed as a promising capability having the strong potential to broaden and deepen our understanding of the most pressing intelligence issues” (Edwards 2014, 1). The Air Force analysis mission technical adviser stated, “Big data analytics provide significant benefits in discovery- the identification of patterns, trends and anomalies which otherwise might be hidden in the noise of everyday event” (Edwards 2014, 2).

It was the commercial companies that pointed out some key problems that the military is facing with these goals of analyzing all this big data. While the commercial sector is leading this issue on how to analyze big data they are aware of some of the pitfalls our militaries face. Peter Tran, senior director of the worldwide advanced cyber defense practice at RSA, commented that “Historically, the intelligence community has suffered from what is termed as ‘operational thrashing,’ where analysts are overwhelmed with the sheer volume of unstructured data, aged intelligence and circular reporting, making real-time accurate decision support extremely difficult, resulting in intelligence analysis paralysis” (Edwards 2014, 1). The Chief Executive Officer of Telum informed with a similar statement while the military representatives foreshadowed this problem for their services.

Another article which touches on a different problem with big data other than data overload, is written by Grace Jean in *National Defense* magazine. This article highlights a problem with the Navy’s bandwidth capability to handle the volume of data they are asking. This is an overlooked problem in the Navy. With the majority of Navy sensors being tactical and having limited bandwidth capabilities there needs to be an agreement within Navy on how much data should be stored on a platform and how to prioritize the data. The challenge this presents to the Navy is how to move information whether it is satellite-based, line of sight-based, or within networks aboard ships to analyze the data. Due to bandwidth constraints a lot of data will "drop to the floor" if automation of data processing and analysis cannot be done (Jean 2011, 41).

Another problem with the movement of analysis on big data for the Navy is one of cultural change. As pointed out in "A Holistic Approach to Intelligence, Surveillance, and Reconnaissance," many individuals and organizations have not fully kept up with the rapid shift in data sharing, distribution, and ways of thinking about and treating information. The military needs to embrace emerging technology culturally, engage with the younger generation, and change how it looks at intelligence and inelligence surveillance reconnaissance by fully incorporating intelligence into operations (Anderson 2011, 59).

This article also highlights the fact that an intelligence surveillance reconnaissance network is not being developed with our partner nations. *The Quadrennial Defense Review Report* notes that both intelligence surveillance reconnaissance and capable partner nations are critical to the new security environment. Although the report mentions that investments in airborne intelligence surveillance reconnaissance will contribute to US capacity for security forces assistance missions, it does not emphasize the key role that intelligence surveillance reconnaissance can play in building partner nation capacity and improving relations with those countries (Anderson 2011, 60).

Applying a more holistic approach to our data sharing with partner nations has significant impact. During a time when manpower is limited, having a partner nation assist with the analysis on the ISR sensor data could prove worthwhile not only for time constraints, but to get a different perspective on the information and increase the overall picture needed for decision superiority.

Summary

Based on the different naval literature and commercial literature available it is easy to decipher that big data is a reality. Navy ID recognizes the need for collection and storage of big data for their decision-making; however, it lacks a coherent plan on how to apply analytics to this data for their decision making and sensor management based on this review of literature.

The commercial industry has made big data analytics a cornerstone of their business practices after realizing the value added that the analytics bring to their revenue stream. The commercial industry has also realized that it does not increase their bottom-line if they cannot offer solutions to what their customers need. This is a major difference in the way Navy and commercial sectors are handling their big data problems.

Sailors and commanders are the customer in the Navy's data collection scheme of maneuver. Sailors need the tools and capabilities to sift through data to provide accurate information to the commander. The commander needs the data provided from the sailors in order to make the most accurate decision possible. The roadmaps and visions documented by Navy ID leadership do not spell out in any detail how they will implement analytical tools for their sailors, nor do they offer up a roadmap to guide sailors in discovering what data truly matters for commanders to make decisions and what the art of the possible is in using this data.

The commercial world does not develop analytics on big data based on possible volume of collection or what the organization wishes to collect. They build the analytics based on what the customer needs to increase their bottom-line and determining what data is important in the decision making process. This approach allows an organization to not waste resources on data that is not needed or toolkits that are insufficient in analyzing what their workforce requires.

Conclusion

The next three chapters will outline the research and design methodology being applied to the thesis problem, analysis, findings, and recommendations for further research. The categories of this literature review will be the primary categories for the research and design as it allows compartmentalizing the different areas of focus within Navy ID strategy and assists with answering the secondary questions presented in this thesis.

CHAPTER 3

RESEARCH METHODOLOGY

Overview

This thesis seeks to understand if Navy ID is implementing the correct strategy to deal with the vast quantity of data that it collects to achieve decision superiority. First, a literature review was conducted in order to establish a solid background of the Navy ID strategy. Areas of study will be national policy documents, Navy ID strategic documents, commercial technology, and problems that the military services are facing to get a handle on big data.

The research consists of three parts. The first focuses on current ID structure, policy, and goals that consists mainly of executive-level strategic documents issued by the senior leadership of the US Navy ID community. By studying these documents, a qualitative judgment on progress in ID is made. ID is a dynamic area. If ID thought and processes are maturing from one strategy to the next, then follow-on strategies should build upon past successes or focus on new aspects of the challenges and goals they need to meet to succeed. Conversely, if no progress or advancement in strategy and policy occur, then one could expect the strategy to remain the same.

Second, research will focus on determining whether Navy ID is innovating within their organization and analytical advances. Studying this will enable the researcher to determine if Navy ID is organizing to meet their goals and objectives and to see if they are placing too much or too little emphasis in a particular area. The third part will examine current commercial application of new analytic technology for better results on big data.

Design Methodology

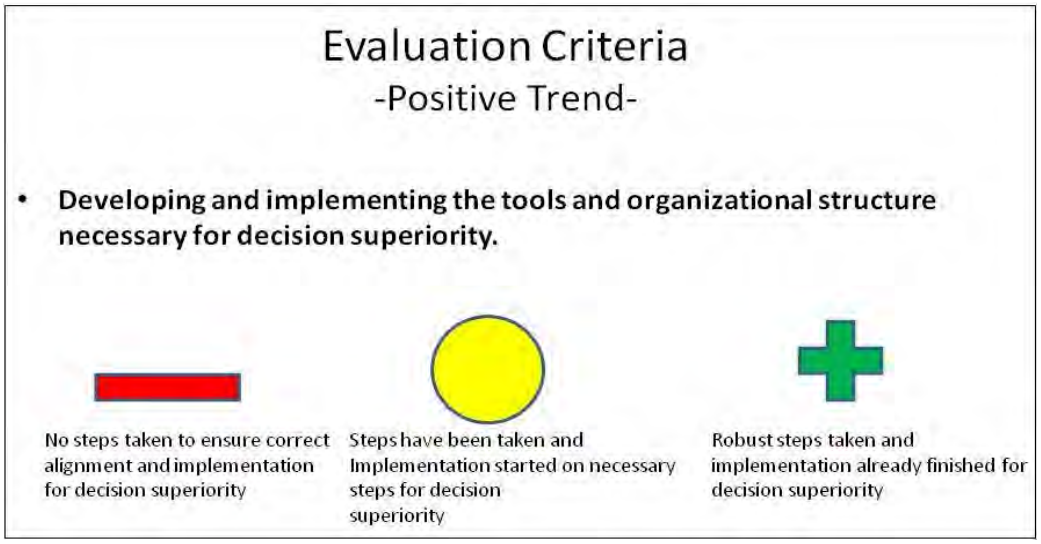
The design methodology used will be a meta-analysis to enable the primary question to be answered by looking into the secondary questions of this thesis. The primary research question posed is: Is Navy ID implementing the correct strategy with their platforms, sensors, and networks interconnected to ensure decision superiority through robust analysis of data? The secondary questions that must be answered in order to answer the primary question will be analyzed through the three-part process mentioned above.

To assist in answering the secondary questions, this thesis will use the evaluation criteria model framework found in from Dr. Jack Kem's book*, Planning for Action: Campaign Concepts and Tools*. The evaluation of criteria framework seeks to determine overall success of the Navy ID strategy by framing the problem to look for gaps in the strategy. Problem framing involves identifying and understanding those issues that impede progress toward the desired end state (Kem 2013). Each secondary question will be compared against this framework to determine where it fits. Using the framework from Dr. Kem's book the critical factors for evaluation and evaluation criteria are annotated in table 1.

Table 1. Critical Factors Being Evaluated

Critical Factors Being Evaluated	Sub-Optimal (-)	Neutral (0)	Optimal (+)
Policy and Strategy			
Organizational Structure			
Commercial Innovation			
Number of Databases and Volume of Sensor Data			
Analytical Methods			

Source: Created by author.



Evaluation Criteria

-Positive Trend-

- **Developing and implementing the tools and organizational structure necessary for decision superiority.**

No steps taken to ensure correct alignment and implementation for decision superiority

Steps have been taken and Implementation started on necessary steps for decision superiority

Robust steps taken and implementation already finished for decision superiority

Figure 3. Evaluation Criteria

Source: Jack Kem, *Planning for Action: Campaign Concepts and Tools* (Fort Leavenworth, KS: Command and General Staff College, August 2013), B-6.

Each critical factor will be evaluated within table 1 which will provide a full evaluation of the secondary problems in relation to the primary question. This will enable the research to determine if there are any gaps in the strategy and where emphasis should be placed to mitigate these gaps.

Threat to Validity

A study is valid if it measures what it claims to, and if there are no logical errors in drawing conclusions from the data. The researcher of this study acknowledges that two external threats to validity exist. External validity has to do with possible bias in the process of generalizing conclusions from a sample to a population, to other subject populations, to other settings, and/or to other time periods (Garson 2014, 3). The researcher in this study is not privy to all the strategy and documents available during this study since a large portion of the Navy IDC operates at the Top Secret Sensitive Compartmented Information level. This may prevent the researcher from accurately depicting what current technology and strategies are being applied in the Top Secret Sensitive Compartmented Information domain.

Another external threat to validity is the rate of change that the Navy ID is faced with in dealing with this problem set. Due to the continuous evolution of the Navy ID community, their strategies and taskings are constantly moving.

The researcher also acknowledges an internal threat of validity to this study. Internal validity has to do with defending against sources of bias arising in research design, which would affect the cause-effect process being studied by introducing covert variables (Garson 2014, 5). The researcher has been a professional officer within the Navy ID community for fourteen years and has a bias towards certain areas of this study.

As the researcher tries to minimize the bias for the study it still must be noted that it exists.

Conclusion

This chapter outlined the research methodology for this study by identifying the type of research, evaluation criteria, and how the author will answer each secondary research question. The analysis of current policy, information from the centers of Navy ID, and information from technology currently being applied elsewhere provide the necessary data for analyzing and evaluating the ability of decision superiority for Navy ID. Chapter 4 will provide the data, analysis, and evaluation of the material outlined in this chapter, in order to answer the primary and secondary research questions.

CHAPTER 4

DATA PRESENTATION AND ANALYSIS

> Information Dominance enables end-to-end defense and management of Navy networks and the information and knowledge that is transported by those networks. The Navy's information capabilities and info-centric communities place the Navy in a better position to meet the challenges and threats of the Information Age. Success in the Information Age will require unmatched mastery of the capabilities, tools and techniques that enable us to collect, process, analyze and apply information.
>
> — Admiral Jonathan W. Greenert, *US Navy Program Guide 2012*

Structure, Policy and Goals

In January 2012, Secretary of Defense Leon Panetta stated, "Modern armed forces cannot conduct high tempo, effective operations without reliable information and communication networks and assured access to space and cyberspace" (Panetta 2012, 5). Within twelve months of that statement, the US Navy began rolling out their strategies and visions within the ID community on what they wanted their personnel to do.

Published in November 2012, the first three documents, *Navy Strategy for Achieving Information Dominance, 2013-2017; Navy Cyber Power 2020;* and *Navy Information Dominance Corps Human Capital Strategy 2012-2017* were intended to set the course for the IDC workforce. They set objectives and goals, establish policy, and provide structure on what Navy ID should be focused on within their commands. On one hand, this is very showing on how serious the Navy ID leadership is on applying ID as a true warfare discipline, at the time of these publications there was no central control organization for carrying out the tasking. The majority of the tasks involved in reaching the goals laid out in these documents were fragmented across multiple organizations that did not have any vertical or lateral chain of command structure with one another.

Since all three documents were published on the same day, it is not possible to determine if they build off one another or have led to successful implementation of the previous strategy. However, all three share the same goals and objectives, which is an excellent start. In this author's opinion, too often military strategy documents are released and unintentionally contradict each other or spell out different goals and objectives to the same audience.

In reviewing the strategy that came out four months after the above three, one can decipher where gaps are starting to widen. The *Information Dominance Roadmap 2013-2028* summarizes the operating and information environments expected during the 2013-2028 timeframe and depicts Navy's required future ID capabilities (Leigher 2013, 2-6). This document describes in detail of what is needed in both short and long term for the three core fundamental ID capabilities of Assured Command and Control, Battlespace Awareness, and Integrated Fires. This document also highlights the areas that need development to achieve success in the core capabilities. In almost every area that speaks on needing to collect the data, analyzing the data, and making decisions of the data it is also stated that Navy ID is not prepared to complete those tasks in their current design.

Information Dominance Roadmap 2013-2028 levies additional tasks on Navy ID to try to close these gaps, but may have been too late in doing so as the other three strategies hit the street four months prior. This document, *Information Dominance Roadmap 2013-2028,* should have been the first strategy out of the gate for Navy ID in order to allow the other three strategies to fill the gaps with additional detail and tasking.

It is also not beneficial that this document levies tasks to close those gaps, yet does not sanction one organization responsible for overseeing these tasks.

Organizational Innovation

Since its inception, Navy ID has had to rely on the Type Commands (TYCOM) or other warfare areas to acquire the resources they needed for their mission. This was an adequate approach until the Navy IDC stood up officially in 2009 and inherited a much greater role in Navy operations and tasking. This required a need for a new organization to take care of their personnel and resources. The Navy decided to innovate by establishing a TYCOM for their newest warfighting community called Information Dominance Forces in October 2014. Figure 4 depicts the old TYCOM structure while figure 5 depicts the new structure.

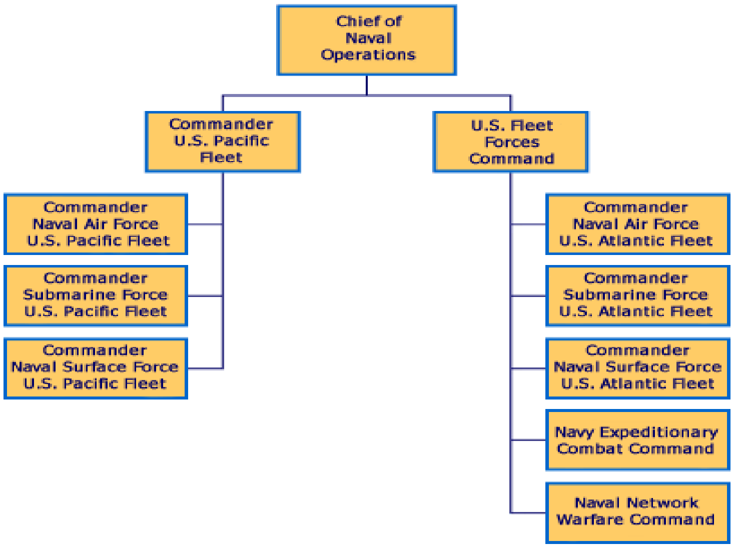
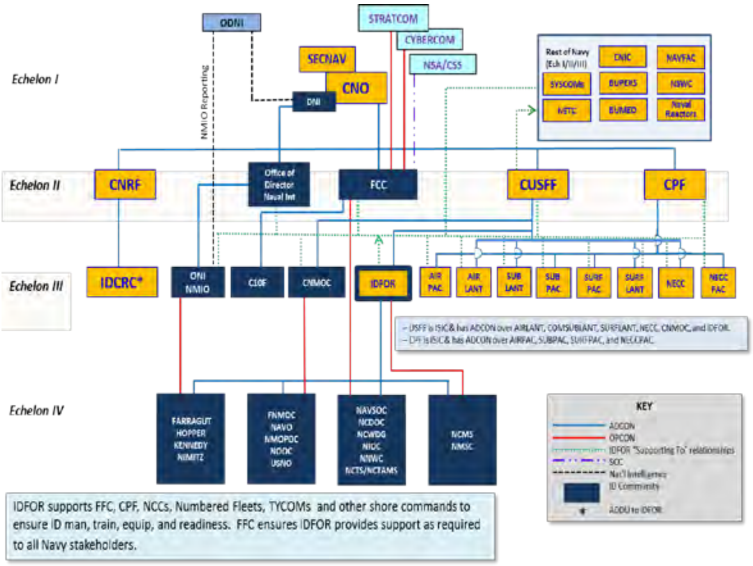

Chief of Naval Operations
Commander U.S. Pacific Fleet
U.S. Fleet Forces Command
Commander Naval Air Force U.S. Pacific Fleet
Commander Submarine Force U.S. Pacific Fleet
Commander Naval Surface Force U.S. Pacific Fleet
Commander Naval Air Force U.S. Atlantic Fleet
Commander Submarine Force U.S. Atlantic Fleet
Commander Naval Surface Force U.S. Atlantic Fleet
Navy Expeditionary Combat Command
Naval Network Warfare Command

Figure 4. Past Navy TYCOM Structure

Source: US Navy, “The Type Commands,” 2014, accessed September 20 2014, http://www.navy.mil/navydata/organization/tycoms.asp.



– USFF is ISIC & has ADCON over AIRLANT, COMSUBLANT, SURFLANT, NECC, CNMOC, and IDFOR.
– CPF is ISIC & has ADCON over AIRPAC, SUBPAC, SURFPAC, and NECCPAC.

IDFOR supports FFC, CPF, NCCs, Numbered Fleets, TYCOMs and other shore commands to ensure ID man, train, equip, and readiness. FFC ensures IDFOR provides support as required to all Navy stakeholders.

Figure 5. “To Be” TYCOM Structure

Source: Ted N. Branch, “Information Dominance” (DCNO All Hands Presentation, San Diego, CA, February 13, 2014), slide 13.

The innovation within Navy’s organization is critical in this manner. From a man, train and equip perspective the Navy IDC was fragmented across the Office of the Chief of Naval Operations, Fleet Cyber Command, Office of Naval Intelligence, Naval Meteorology and Oceanography Command, Navy Cyber Forces, and the platform TYCOMs. Attempting to make these disparities more efficient through Memoranda of Understandings and Memoranda of Agreements, without a centralized organization for man, train and equip responsibility and accountability became increasing problematic since the stand-up of the Navy IDC. Due to the fragmentation of offices that were accountable for separate pieces, the IDC never efficiently integrated with the required functioning process to meet the fleet’s readiness kill chain.

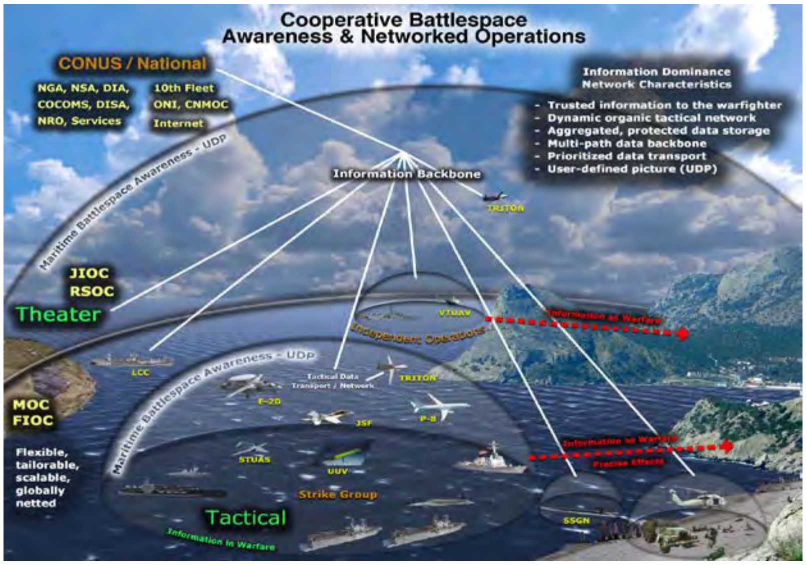
The innovation of the Information Dominance Forces TYCOM is the answer for the establishment of a single, integrated TYCOM that partners not only with the fleet but with the rest of the Navy. Since the network in the Navy is nearly universal across the Navy, as a battlespace, extends well beyond the responsibility of the Fleet. Therefore, to be most effective, this TYCOM's portfolio must necessarily include Navy's shore components as well as its afloat commands.

Office of the Chief of Naval Operations, Fleet Cyber Command, Office of Naval Intelligence, and Naval Meteorological and Oceanography Command have identified manpower and resources that will transfer to the new command. The ID TYCOM will have administrative control of the man, train and equip functions of each ID echelon IV command which is needed to properly execute the goals in the Navy ID strategies and roadmaps. The TYCOM's mission will be to provide the capabilities and workforce necessary to maximize Navy readiness and support Navy ID operations. This mission includes capabilities associated with networks, cyber, space, intelligence, meteorology, oceanography, hydrography, cryptology/signals intelligence (SIGINT), electronic warfare, and the electromagnetic spectrum (Branch 2014b).

Navy ID continues to innovate through organization to accomplish their goals and objectives for their vision. Another organizational innovation Navy ID has developed is the standup of the Navy Task Force Cloud in January 2014. The purpose of the task force is to ensure the Navy continues to employ information to their operational advantage, combat the threats posed by those who seek to rob Navy of that advantage, and deal with a shrinking resource base. The Task Force Cloud Charter also points out how the Navy must take advantage of the technology now available and rethink their processes as they move from being a system-centric force to a data-centric force (Branch 2014a, 2).

Analytical Vision

Navy ID leadership graphically and verbally has shared their analytic vision in regards to the battlespace for both analytical analysis and sensor management. Figure 6 depicts the graphical end state of what Navy ID leadership portray. Figure 6 is the end state Navy ID is trying to achieve where every platform is a sensor, all sensors are interconnected, and decisions on the data being shared can be made in real time.



Cooperative Battlespace Awareness & Networked Operations

Information Dominance Network Characteristics

- Trusted information to the warfighter
- Dynamic organic tactical network
- Aggregated, protected data storage
- Multi-path data backbone
- Prioritized data transport
- User-defined picture (UDP)

CONUS / National
NGA, NSA, DIA, COCOMS, DISA, NRO, Services
10th Fleet ONI, CNMOC Internet
Maritime Battlespace Awareness - UDP
Information Backbone
TRITON
JIOC
RSOC
Theater
VTUAV
Information as Warfare
Independent Operations
LCC
Maritime Battlespace Awareness - UDP
Tactical Data Transport / Network
TRITON
E-2D
JSF
P-8
MOC
FIOC
Flexible, tailorable, scalable, globally netted
STUAS
UUV
Information as Warfare
Precise Effects
Strike Group
SSGN
Tactical
Information in Warfare

Figure 6. Navy ID End State

Source: Ted N. Branch, “Information Dominance” (DCNO All Hands Presentation, San Diego, CA, February 13, 2014), slide 24.

In spring of 2014, Admiral Ted Branch, Director of Naval Intelligence/Deputy Chief of Naval Operations for Information Dominance acknowledged what the end state should look like for analysis on the data Navy needs to analyze when he stated:

> Computers, communications links, encryption devices, and other IT allow our Navy Commanders to correlate data, make decisions based on that correlated data, issue orders to the subordinate forces responsible for carrying-out those decisions, assess the effects achieved through subordinate actions, and report the outcomes to higher headquarters. Put simply, they enable the vital business of Command and Control (C2). (Branch 2014c, slide 14)

Both the graphic and statement by Admiral Branch describe what the end state is supposed to look like, and there is little counter argument for the need to look different. In order to accomplish both of these representations there needs to be a focus on analytics of the data for both the sailor and the system.

It is at the level below the Deputy Chief of Naval Operations for Information Dominance where the analytical vision seems to be getting lost. In an article by Navy ID leadership authored in July 2014, they reference the famous *Art of War* author Sun Tzu: “Know the enemy, know yourself; your victory will never be endangered. Know the ground, know the weather; your victory will then be total.” This was a reference to speak about the need for Navy ID to have battlespace awareness for optimal decision-making ability. As the article talks about knowing the enemy, it tries to distinguish between intelligence and information by stating:

> That is precisely what distinguishes ‘intelligence” from “information.” Whereas “information” largely consists of facts and data exchanged between users and consumers, “intelligence” requires deliberate, active, targeted collection, rigor of analysis, and prompt dissemination that yields a decisive advantage to a decision maker. (White and Filipowski 2014, 30-35).

It is here where the analytical vision and what is needed to achieve decision superiority is semantically challenged. All intelligence is information and all information is needed. The users and consumers of the information should be the personnel responsible for determining what is the intelligence value of the information. When reviewing all the amounts of data the Navy plans to collect, if you distinguish between 'information' and 'intelligence' as the authors above have, an analyst will begin analyzing in a stovepipe and not have all relevant information to assist in determining the intelligence value of that information. If analytical systems are not designed with pre-determined analytics based off of the customer and user of the data, the analysts will be able to determine very little in assisting the decision making process due to information overload.

Too Much Data

Currently the Navy ID sailors are faced with monumental amounts of data that they have access to, however limited capability to analyze the data in real time or near-real time. As Navy ID pushed for increased Battlespace Awareness they worked both internally and externally with the intelligence community to allows sailors to have more access to databases. On average, this resulted in a sailor in the Navy ID community having access to over 800 databases all containing millions of gigabytes of data, vice approximately twenty databases.

Out of this large set of databases, only a handful are utilizing predictive analytics. This means the sailor is still performing the majority of their analysis by time-consuming rudimentary practices. There will always be a need for the 'human in the loop' when it comes to analysis of data for a decision, but in order to provide a commander the right data to enable decision superiority, it cannot rely soley on a human to operate at machine speeds.

Similar to the problem of being exposed to new data sources, the Navy is increasing by the month the number of organic sensors it is placing in the information environment to bring back the data being collected for analyzation. The organic sensor issue is a two part problem. First, the Navy ID comunities goal as described previously in this thesis in Admiral Branch's analytical vision is to allow the senors to and sailors to sift through the organic data expeditously in order to tip or reprioritize intelligence surveillance reconnaissance systems for better employment against requirements. The second part is to have the ability to merge the organic sensor data with the data from external databases and sensors to datamine for the key piece of information to achieve decision superiority.

This cannot be done without having some type of predictive analytic running on the data being collected from all the organic sensors and external data in a constant fashion. Human analysis cannot keep up at the rate that data changes in the electromagnetic and cyber environment. By the time a sailor has sifted through the information for the critical pieces of intelligence and passed that information on to the commander, the data has changed thereby preventing decision superiority.

A Watch Center Use Case

An example of how general analytical practices are applied within the Navy ID community can be examined through the application of their watch centers. If we take an average watch center you will have a battlewatch captain, who oversees the watch center and their primary job is to make immediate decisions on critical items or to get the information in front of the commander for a decision. You will have a SIGINT position, a cyber position, an intelligence position, a meteorological position, a general naval blue force tracker position and a network position.

These positions while all being maintained by sailors who have been trained for their job are usually inefficient at putting the puzzle pieces of information together to give the battlewatch captain or the commander the holisitc operational picture to make the most accurate decision. Each position has a range of 10-800 internal and external databases it uses to analyze data for the key pieces of information. It is impossible for a human to operate at machine speeds to sift through all this data and also be able to analyze how it impacts the other positions in respect to the problems they are working.

Could certain key pieces of meteorlogical data that is filtering into the desk's databases contain key pieces of critical information that may signal the inability to perform SIGINT at Location A? If that data could have been seen, the SIGINT desk officer could have precoordinated with other assets for SIGINT collection at that time.

Could a key piece of cyber data in the Pacific area of responsibility signal an impending event to our continental US networks based on the historical pattern and trends of the cyber data? This could allow the network officer to implement network defense tactics so continental US networks were not harmed.

While the watch center has sophisticated tools, availability of data, and the ability to task different sensors and platforms, the desk officers perform in stovepipes by nature of the time it takes to analyze the data that continues to overload their desk. As the data grows so does the challenge on extracting insights and avoiding paralysis by analysis for decision making.

Commercial Innovation

An individual only has to pick up their smartphone to see how the commercial sector is innovating on analytics to allow the consumer to make a better decision based on pre-determined analytics. Every choice made within an application on a smartphone or tablet is acknowledged and when starting to type a question into a search engine on that device or looking for a new movie to watch on Netflix, the application starts returning answers based on your past choices. While never 100 percent accurate in real time, what the commercial sector learns with predictive analytics is in fact how to lessen risk. Each negative outcome that occurs presents an opportunity from which to learn, systematically. To this end, the information from which predictive model learns includes the negative, i.e., bad data, as well as the positive, i.e., good data. Even if the information contains more bad data than good data, the other analytical methods can leverage 100 percent of the data in order to learn from all the information.

In an opposite approach to trying to distinguish between 'information' and 'intelligence' as Navy ID leadership is doing, the commercial sector looks at all the information as intelligence for insights like trends, patterns, and outliers that can improve decisions, drive better operations performance, and save millions of dollars.

The major communication companies have similar interests as our Navy ID community. Both are data driven, need to prevent attacks, and have elaborate watch centers to ensure decision superiority, but the commercial world has analytical processes in place to assist in the speed and quality of decisions being made.

As the commercial world builds systems to analyze all their data, they ensure integration and compatibility between the systems so analytics running on one system can tip and alert another system that holds data which contains a critical link. They do this so they constantly understand, predict, and then act. It is not only companies that are known for technology that are taking advantage of predictive analyitcs on their data.

John Deere, a major agricultural company, uses sensors added to their latest equipment to help farmers manage their fleet and to decrease downtime of their tractors as well as save on fuel. The information is combined with historical and real-time data regarding weather prediction, soil conditions, crop features, and many other data sets. They are doing this to assist farmers in determining which crops to plant where and when, when and where to plow, where the best return will be made with the crops, and even which path to follow when plowing. All this will increase the productivity and efficiency of the crops that will in the end lead to higher production and revenue (DataFlow 2014).

Commercial Similarities

The commercial industry and US Navy do have similarities as it pertains to organizational level leadership. Both sides implement similar senior leadership to spearhead implementation of technology advances. This can be seen at the leadership level of Chief Information Officer, Chief Technology Officer, and Chief Operating Officer. These three positions in the senior leadership level work together on deciding what technological advances to implement, the reasons why, and how to exploit the positive gains from the implementations for better customer satisfication.

Research and Development (R&D) is another area where US Navy and the commercial world parallel one another. Both industries have built in R&D within their organizations. Both industries leverage one another by looking at what the other sector has developed and then rsearching how to implement that idea into their own practices if deemed sufficient for forward movement. In 2012, the US Navy and Marine Corps spent $17.7 billion in R&D. This large number needs to take into account all of the different platforms the US Navy and Marine Corps must research and develop for and cannot be viewed as comparable to a single commercial corporation. However, once the number is broken down into the different areas the US Navy and Marine Corps focuses on, it can be viewed on the scale of a mid-level corporation R&D budget.

It is at the implementation point of an R&D solution where the US Navy and the commercial world begin to separate on their uses for advanced technology and differences can be seen. These differences vary between internal and external factors.

Commercial Differences

While the commercial world can implement a solution right away to impact their customers, the US Navy is handicapped through the federal acquisition program. This thesis will not discuss the complexity of the federal acquisition program, it will only highlight the fact that once a US Navy R&D solution has been found, it can take an average of two to five years to implement due to the federal acquisition guidelines. This means that when a Navy customer, commander and sailor, are afforded the opportunity to utilize this technological advantage it is already outdated.

This outdated technology, in relation to predictive analytics is a very big problem that US Navy ID leadership needs to solve. If US Navy collection systems are leveraging software and hardware commercial technology for their data collection needs, the new technology implemented by US Navy R&D is incompatible with the commercial technology due to continuing advances and updates the commercial world is making to their products. At times this incompatibility renders a step backward in predictive analytics in a real time environment for the US Navy ID community since they end up doing additional work with both products to work towards a solution. This directly impacts the speed at which a smart decision can be made.

Another noticeable difference is the interaction between the R&D departments of both organizations and their customer base. The commercial industry is in a constant feedback loop with their customer base as almost every product or application has review submittal forms, software feedback, or a number of different feedback mechanisms to allow the R&D teams to improve glitches, shape the technology to what the customer really needs, and make itself more compatible and dependable. This dramatically improves performance and decision making in the analytic realm as the more data available, regardless of type and source, is all fused to provide a greater awareness of the decision needed to be made.

In the US Navy ID community these feedback mechanisms are scarcely built into systems or organizations. When feedback is given it is usually in the form of an email from one operating unit to a higher level unit and then gets forwarded on several more times, if approval from each level it passes is given, before reaching the R&D departments.

The latency of fixing a glitch or collecting a new data set for the system does not end with the email chain. Again, due to acquisition program management regulations a software glitch that can be fixed with a patch in a few minutes to days, on average takes about six months to finish and get back to the system of the originating unit.

Secondary Answers

The above analysis and findings allows for the critical factors to be evaluted to assist in answering the secondary questions. Table 2 depicts where the research has placed the US Navy ID critical factors. The critical factors evaluated help answer the secondary questions.

Table 2. Critical Factors Evaluated

Critical Factors Being Evaluated	Sub-Optimal (-)	Neutral (0)	Optimal (+)
Policy and Strategy		0	
Organizational Structure			+
Commercial Innovation	-		
Number of Databases and Volume of Sensor data			+
Analytical Methods	-		

Source: Created by author.

In answering the first secondary question, does having more data accessible to a naval unit allow for an easier management of sensor employment against requirements and enhanced Battlespace Awareness; the answer is no. While the US Navy ID community is optimal in the way they are organizing their community, the number of databases and sensors they have, neutral on implementing their policy to align with strategic level policy they fail to achieve success in the categories that matter most for this question.

Having the analytical methods in place to provide the sailor and commander what they need for decision superiority is the crux for this question. Without the toolkits availble to sift through all the data a naval analayst is faced with, the analyst is trapped in an information overload scenario. This actually detracts from having enhanced battlespace awareness and prevents the ID community from managing their sensors correctly. Without the proper analytics one is not seeing the entire battlespace to assist in making the decision on where to employ sensors. This leaves requirements unfilled and detracts from decision superiority.

The other part which assists in rendering a negative value to this question is leveraging of commercial innovation. While part of that is an external factor of acquisition and program management timelines the Navy ID has limited influence on, it is still a fact that cannot be changed. Too often the technology being placed on US Navy platforms is outdated and incompatible with the rest of the commercial world. The feedback mechanism on software and hardware improvement is also a negative value which prevents problems from being known soonest and remedied.

The answer to the next secondary question, is there current technology now that the Navy should be leveraging, is yes. As researched in this thesis there is a multitude of available technologies for predictive analytics and decision making that should be leveraged. All major commercial industries are taking advantage of these technologies and implementing them for greater gains in revenue and customer satisfaction. The US Navy ID is organizationally set up to streamline the implementations of these technologies, however they are lacking on the needed action at this time. Being more aggressive on leveraging commerical innovations would also bring the US Navy ID more in line with their own strategic policies and vision and national policies and vision as both sets call for leveraging commercial innovations.

In answering the final secondary question to determine if the current US Navy ID strategies assist or hinder the naval analyst in viewing the battlespace; the answer is both. In looking at the critical factors one could assume that optimal organizational structure, a large volume of sensors and databases, and neutral strategy and policy that the US Navy ID strategy ultimately enhances the naval analyst in viewing the battlespace. From those critical factors, then yes, the ID strategy is working. However, the ID strategies fail to mention the use of predictive analytics often enough within their strategies for decision superiority that it is not equated into tasking for the community. The other negative part of the strategy is too often the cyber domain is separated from the electromagnetic spectrum domain when in reality the electromgantic spectrum and cyber domains leverage one another. This separation has led to different systems being built for the two domains even though the systems are capable of doing the same mission. In this aspect with the above, the strategy is not assisting the naval analyst from viewing the battlespace.

Conclusion

By evaluating the critical factors and answering the secondary questions it allows for a conclusion to be made on the primary question. Is the Navy ID community implementing the correct strategy with all their platforms, sensors, and networks interconnected to ensure decision superiority through robust analysis of data? This is both a yes and no answer.

By looking at the secondary questions the strategy has aligned the ID community organizationally capable and streamlined and fused the different skillsets that are needed to work with one another which is the first step that must be taken. The senior leadership in the ID community has articulated the vision for the end state of their strategy in a precise manner. The US Navy ID community is also networking their platforms and sensors, gaining more access to databases and external sensors which is all optimal for the US Navy ID in achieving success in their strategy.

Looking at the other critical factors evaluated in answering the secondary questions it can be determined the strategy is not being implemented correctly. The lack of emphasis on the predictive analytics to allow for enhanced battlespace awareness and sensor management is a factor that must be instituted within their strategy. While our data gathering sensors are being overwhelmed by information, we must realize our analysts are being overwhelmed as well by information when trying to make a decision.

One gap seems to be the manner in which elecromagnetic spectrum and cyber domains are treated as separate entities rather than complementary domains. This is not the case at the senior leadership levels or with analysts doing the work, but in the organizational level between the two the strategy does not seem to resonate. This may correct itself while the new organizational structure has had more time to operate, but still must be noted.

Finally, the lack of the ability to leverage commercial innovations at a pace needed for today's threat environment needs to be addressed within the strategy to enable success. For the Navy ID community to be successul in decision superiority, they must have all their critical factors synchronized correctly. Chapter 5 will provide several recommendations that may be of assistance in mitigating the gaps in the strategy.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

> To create a single electronic warfare network linking everything from subs to drones, . . . the challenge is bringing all that together, understanding it, controlling it, so you can actually use it. That's a lot of work left to be done.
>
> — Captain Rob "Ice" Gamberg, "New Electromagnetic Maneuver Warfare Strategy Emerges"

Introduction

This thesis set out to answer the primary research question: is the Navy ID community implementing the correct strategy with all their platforms, networks, and sensors to ensure decision superiority? In order to answer this question several secondary questions were answered: (1) Does having more data accessible to a naval unit allow for an easier management of sensor employment against requirements and enhanced Battlespace Awareness?; (2) Is there current technology available now that Navy ID should be leveraging?; and (3) Does the current Navy ID strategy assist or hinder the naval analyst in viewing the battlespace?

None of the answers provided a clear concise agreement on a definitive yes or no. However, the answers did provide enough information to determine gaps in the current strategy and recommendations for future research or future mitigation strategies.

Conclusion and Recommendations

While national and operational strategy, policy, and documents share the same common themes there does seem to be a piece missing between the Navy ID operational strategy and how this strategy is integrated within the tactical/analytical units of the ID community. This is seen very clearly in the watch center use case and at the mid-grade organizational level of how the electromagnetic spectrum and cyber domains are treated separately. Until the organizational level aligns with higher headquarter strategy on electromagnetic spectrum and cyber domains there will continue to be a gap that keeps the analysts stove-piped and hinder the commander's decision making process.

One recommendation would be to ensure the mid-grade level officers in charge of implementing these strategies understand the distinct differences and similarities between these two domains. This will enable the organization to leverage their systems and toolkits more adequately to provide better decision-making abilities. In order to accomplish this, the Navy IDC must begin teaching this at the earliest opportunity for their workforce. If not, the result will be mid-level leaders who do not understand how a simple personal communication device is tied into their cyber and space assets and will consistently miss opportunities for the home field advantage the Office of the Chief of Naval Operations N2/N6 director continues to pursue.

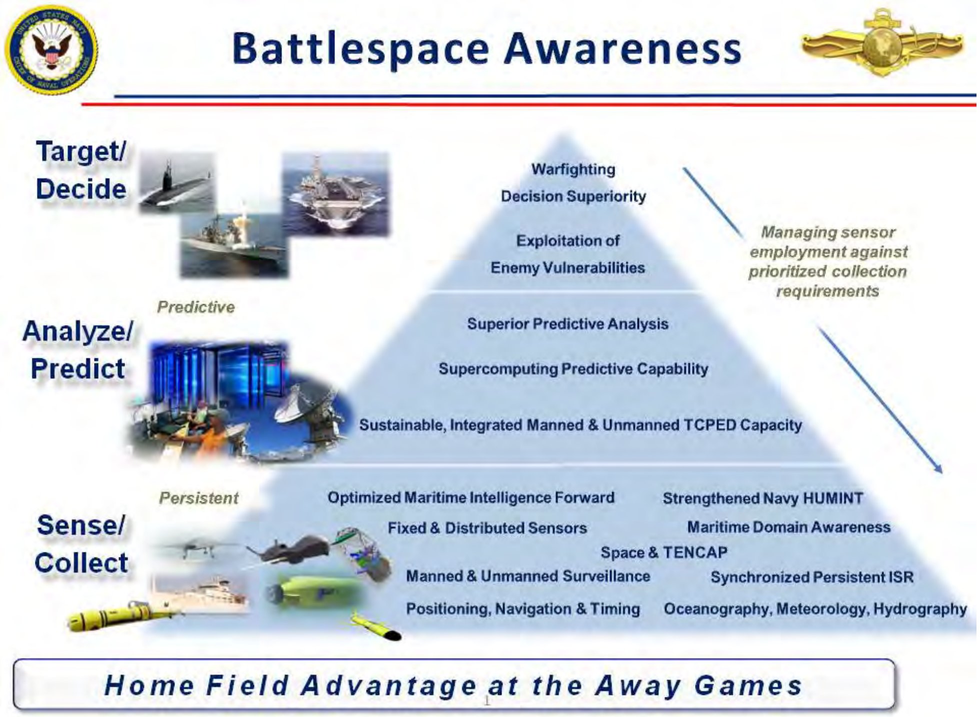
Leveraging commercial technology must be done at every level of the Navy ID chain of command. The rate of change at which commercial technology on big data is evolving and the rate of distribution at a low cost to our adversaries on these technologies emphasize the need for the Navy ID community to becoming a full-fledged partner with commercial innovation. The gap here is between how the Navy ID community and commercial industry view data.

The commercial sector views all data as good data. What the Navy would filter out of their collection systems as 'bad data' is good data in the commercial world. This is because even 'bad data' which may be geolocation errors, spelling errors, fabricated lies all assist in the overall data collection in determining what the best decision is. This divergence in thinking between the Navy ID community and commercial sector is a major factual reason as to why Navy ID is not progressing much more than where they were five years ago; even though they have much more information at their fingertips than ever before.

To close this gap, the Navy ID community needs to stand up an office whose job is to research these commercial initiatives and leverage current opportunities through the agile solutions to implement the technology quicker. They must also divest themselves of being so closely tied to Office of Naval Research, US Naval Research Laboratory, Program Executive Offices and other large bureaucratic organizations that implement technology at the rate of what was needed five years ago. This is not to say they do not need these organizations, but the relationship must be revamped to allow greater commercial technological innovations to permeate throughout the Navy ID community faster by forcing systems designed with open source and standards, platform-agnostic solutions, and pace technology and the threat.

The most critical gap within this research is noted between the developer and customer at all three organizational levels; strategic, operational and tactical. While strategically, organizationally, and amount of data accessibility is tracking on a positive course, it does not seem that anyone is involved in ensuring the analyst has what they need to support the commander. Without closing this gap, the entire strategy will never be implemented to the fullest and decision superiority will never be reached.

The Battlespace Awareness graphic below depicts how Naval warfighters will find, penetrate, and predict the enemy by making better decisions faster than our adversaries. The mechanisms of sensing, collecting, analyzing, predicting, targeting and deciding graphically depicted below show how decision superiority will be accomplished within Navy ID's future. To this end, the analyst must be given the tools and capabilities they will need to handle the overload of information.



Battlespace Awareness

Target/ Decide

Warfighting Decision Superiority

Exploitation of Enemy Vulnerabilities

Managing sensor employment against prioritized collection requirements

Predictive

Analyze/ Predict

Superior Predictive Analysis

Supercomputing Predictive Capability

Sustainable, Integrated Manned & Unmanned TCPED Capacity

Persistent

Sense/ Collect

Optimized Maritime Intelligence Forward

Strengthened Navy HUMINT

Fixed & Distributed Sensors

Maritime Domain Awareness

Space & TENCAP

Manned & Unmanned Surveillance

Synchronized Persistent ISR

Positioning, Navigation & Timing

Oceanography, Meteorology, Hydrography

Home Field Advantage at the Away Games

Figure 7. Battlespace Awareness Decision Making

Source: Ted N. Branch, "Information Dominance" (DCNO All Hands Presentation, San Diego, CA, February 13, 2014), slide 16.

In order to enable the commander to make the best decision and allow the analysts to take advantage of all the possible data they could touch, the Navy ID needs to ensure they are in lock step with the needs of the customer. While the standup of Task Force Cloud is a right step to determine big data needs within the Navy, a better step would be to gather this information from the analysts.

This would assist in ensuring the data coming into databases and toolkits is the correct data needed for decisions, allow for analysis on this data to determine what other sources would be of benefit, complimentary, and reduce manpower and money spent on bringing in data sources and analytical methods that the customer does not want. This would also force a breakage in the stovepipe architecture within a watch center as the analysts are forced to determine how each other's data sources fit into the overall decision.

Working more in line with the commercial world and studying their use cases could better help the Navy ID community in closing this gap. The majority of successful use cases studied in the commercial world with using predictive analytics and big data all start with determining what the customer needs.

Future Research Topics

There are many areas that this thesis did not address, that impact the future of implementing the Navy ID strategy. These areas would give additional insight on limitations and capabilities of current Navy ID disciplines along with determining other gaps that would impact implementation these strategies.

One area for further study is bandwidth capability on naval platforms. Since the naval platforms are not fixed sites that can have dedicated fiber and dark runs into them, they are usually limited greatly on their bandwidth across the different afloat network domains. Studying bandwidth constraints and how this relates to bringing in data for the analysts and offloading data to another organization is a key concern.

Looking at bandwidth in a denied communications environment is an area that needs further discovery. When a naval platform is ingesting data organically in a denied communications environment and suddenly reconnects back to the network, there are no prioritization mechanisms for what data comes in or is offloaded first.

Another area of study that needs to be researched is what joint options are currently available. With a national policy driving the military to operate more in a joint environment, the need to leverage each service's capabilities is required. This assists in reducing the manpower and resources needed to build something new that is already complete within another service and affords an opportunity to determine how to align each different service's data to complement one another. This is also related to the above research topic of bandwidth utilization.

The last research topic that could be looked at for future research is the use of unmanned systems as a predictive analytic itself along with the ability to be a bandwidth implementation node. Unmanned systems are increasing each day within the Navy and collecting more and more data through their sensors. This increase in data collection that leads to analysis paralysis could be offset by applying predictive analytics onto the unmanned systems sensors which assist the analysts in what they need and assist in determining future reactions by the unmanned sensor.

Summary

In an article Admiral Jonathan Greenert wrote for *Breaking Defense,* he summed up the importance of the topics touched in this thesis:

> We will improve our awareness of the EM and cyber environments. We will detect and assess in real time what is happening in the EM and cyber environment, predict how the environment will react and use this knowledge to guide our own actions. Building this level of awareness will be challenging. Our tools for collecting and analyzing information in the EM and cyber environment are limited, and we lack the familiarity and understanding to take full advantage of the information we do have. To build better tools for sensing the EM and cyber environment, we will work closely with industry and academic researchers. (Greenert 2013)

REFERENCE LIST

Accenture Federal Services. 2012. *Using Predictive Analytics to Increase Equipment Reliability and Reduce Costs.* Accessed September 15, 2014. http://www.accenture.com/2012/sitecollectiondocuments/pdf/accenture-federal-services-using-predictive-analytics-to-increase-equipment-reliability-and-reduce-costs.pdf.

Air-Sea Battle Office. 2013. *Air-Sea Battle: Service Collaboration to Address Anti-Access and Area Denial Challenges*. Washington, DC: Department of Defense.

Amazon. 2014. "Amazon Kinesis." Amazon Web Services, January 1, 2014. Accessed August 31, 2014. http://aws.amazon.com/kinesis/.

Anderson, Dagvin. 2011. "A Holistic Approach to Intelligence, Surveillance and Reconnaissance." *Air and Space Power Journal* 25, no. 4 (Winter): 54-64.

Automated Insights. 2014. "Big Data Needs Big Insights." August 1. Accessed August 31, 2014. http://automatedinsights.com/resources/Big-Data-Needs-Big-Insights.pdf.

Barlow, Mike. 2013. *Real-Time Big Data Analytics: Emerging Architecture*. Sebastopol, CA: O'Reilly Media.

Branch, Ted N. 2014a. Deputy Chief of Naval Operations for Information Dominance Memorandum, Subject: Task Force Cloud. Washington, DC, January 16.

______. 2014b. "Implementation Planning Team to Prepare for Information Dominance TYCOM Establishment." *CHIPS*, January 16. Accessed September 14, 2014. http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=4884.

______. 2014c. "Information Dominance." DCNO All Hands Presentation, San Diego, CA, February 13.

Card, Kendall. 2012. "Navy ISR Family of Systems: An Integrated Future." Presentation, Navy Information Dominance Industry Day, Chantilly, VA, March 7.

Card, Kendall E., and Michael S. Rogers. 2012a. *Navy Cyber Power 2020.* Washington, DC: Department of the Navy, November.

______. 2012b. *Navy Information Dominance Corps Human Capital Strategy 2012-2017.* Washington, DC: Department of the Navy, November.

______. 2012c. *Navy Strategy for Achieving Information Dominance, 2013-2017.* Washington, DC: Department of the Navy, November 28.

DataFlow. 2014. "John Deere is Revolutionizing Farming with Big Data." Accessed October 21, 2014. http://www.bigdata-startups.com/BigData-startup/john-deere-revolutionizing-farming-big-data/.

Edwards, John. 2014. "Military Intel Turn to Big Data Better Situational Awareness." *Federal Times,* June 2. Accessed September 28, 2014. http://www.federaltimes.com/article/20140602/FEDIT/306020009/Military-intel-turn-big-data-better-situational-awareness#comments.

Garson, David. 2014. "Validity." College of Humanities and Social Sciences, North Carolina State University. Accessed November 23, 2014. http://faculty.chass.ncsu.edu/garson/PA765/validity.htm.

Gambert, Rob. 2014. "New Electromagnetic Maneuver Warfare Strategy Emerges." *Interference Technology*, October 30. Accessed February 28, 2015. http://www.interferencetechnology.com/new-electromagnetic-maneuver-warfare-strategy-emerges/.

Greenert, Jonathan W. 2012a. "Imminent Domain." *United States Naval Institute Proceedings* 138, no. 12 (December): 16-21.

______. 2012b. *U.S. Navy Program Guide 2012.* Washington, DC: Department of the Navy. Accessed September 20, 2014. http://www.navy.mil/navydata/policy/seapower/npg12/top-npg12.pdf.

______. 2013. "Adm. Greenert: Wireless Cyberwar, the EM Spectrum, and the Changing Navy." *Breaking Defense*, April 3. Accessed November 23, 2014. http://breakingdefense.com/2013/04/adm-greenert-wireless-cyber-em-spectrum-changing-navy.

Halper, Fern. 2011. *Predictive Analytics: The Hurwitz Victory Index Report.* Needham, MA: Hurwitz and Associates.

IBM Corporation. 2012. *A Business Intelligence Agenda for Midsize Organizations: Six Strategies for Success*. Somers, NY: IBM Corporation.

______. 2014. "Maximize Insights, Ensure Trust And Improve IT Economics." Accessed August 31, 2014. http://www.ibm.com/big-data/us/en/big-data-and-analytics/it-economics.html.

Jean, Grace. 2011. "Drone Sensor Data Will Overload Networks, Navy Officials Warn." *National Defense* 96, no. 693 (August): 40-41.

Joint Chiefs of Staff. 2012. *Joint Operational Access Concept (JOAC).* Ver. 1.0. Washington, DC: Department of Defense, January 17.

Kem, Dr. Jack D. 2013. *Planning for Action: Campaign Concepts and Tools*. Fort Leavenworth, KS: US Army Command and General Staff College.

Konkel, Frank. 2014. “The Details about the CIA’s Deal with Amazon.” *The Atlantic*, July 17. Accessed August 31, 2014. http://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/.

Leigher, William F. 2013. *U.S. Navy Information Dominance Roadmap 2013-2028,* Washington, DC: Department of the Navy, March.

McCafferty, Dennis. 2014. “Surprising Statistics about Big Data.” *Baseline*, February 18. Accessed August 31, 2014. http://www.baselinemag.com/analytics-big-data/slideshows/surprising-statistics-about-big-data.html.

Panetta, Leon E. 2012. *Sustaining U.S. Global Leadership Priorities for 21st Century Defense.* Washington, DC: Department of Defense.

Porche, Isaac. 2014. *Data Flood: Helping the Navy Address the Rising Tide of Sensor Information*. Santa Monica: RAND Corporation.

Progress Software Corporation. 2014. *2014 Data Connectivity Outlook.* White Paper. Accessed August 31, 2014. http://goo.gl/yxp9DI.

Seigel, Eric. 2010. *Seven Reasons You Need Predictive Analytics Today*. San Francisco: Prediction Impact.

Snijders, Chris, Uwe Matzat, and Ulf-Dietrich Reips. 2012. “Big Data: Big Gaps of Knowledge in the Field of Internet Science.” *International Journal of Internet Science* 7, no. 1 (July): 1-5. Accessed August 31, 2014. http://www.ijis.net/ijis7_1/ijis7_1_editorial.pdf.

Swartz, Matthew, and Christopher Page. 2014. “Equipping Commanders in the Information Age.” *United States Naval Institute Proceedings* 140, no. 7 (July): 24-29.

US Navy. 2014. “The Type Commands.” Accessed September 20, 2014. http://www.navy.mil/navydata/organization/tycoms.asp.

US President. 2012. *National Defense Strategy 2012.* Washington, DC: Department of Defense.

______. 2013. *National Maritime Domain Awareness Plan for the National Strategy for Maritime Security.* Washington, DC: The White House, December. Accessed October 5, 2014. http://www.whitehouse.gov/sites/default/files/docs/national_maritime_domain_awareness_plan.pdf.

White, Jonathan, and Sean Filipowski. 2014. “Know the Environment, Know the Enemy, Know the Target.” *United States Naval Institute Proceedings* 140, no. 7 (July): 30-35.